A method to find the volume of a sphere in the Lee metric, and its applications

Sagnik Bhattacharya, Adrish Banerjee
Department of Electrical Engineering, Indian Institute of Technology Kanpur
Email: {sagnikb, adrish}@iitk.ac.in

***Abstract*—We develop general techniques to bound the size of the balls of a given radius r for q-ary discrete metrics, using the generating function for the metric and Sanov's theorem, that reduces to the known bound in the case of the Hamming metric and gives us a new bound in the case of the Lee metric. We use the techniques developed to find Hamming, Elias-Bassalygo and Gilbert-Varshamov bounds for the Lee metric.**

I. Introduction

A. Background

One of the outcomes of Shannon's classic work on information theory is a long and ongoing investigation of point-to-point communication over a discrete memoryless channel and the limits of reliable communication over such a channel. To describe these limits, we can use various metrics defined on the codeword space that are matched to the channel under consideration, where we say that a metric is matched to a channel if nearest neighbour decoding according to the metric implies maximum likelihood (ML) decoding on the channel [1]. The kind of metric chosen can vary, for example, depending on the kind of modulation scheme used for communication over the channel. The limits also change depending on what kind of error criterion is being used - for example, whether we want average error or maximum error to be bounded.

The most well studied metric is the Hamming metric, which is suited to orthogonal modulation schemes [2]. For the error rate to be exactly zero, we have several upper bounds like the low-rate average-distance Plotkin bound [3], the Hamming bound based on sphere packing [2], the Elias-Bassalygo bound [4] and the linear programming based MRRW bound [5], and lower bounds like the Gilbert-Varshamov bound [6] that tell us what rates are possible and what are not, given an error criterion that the code is to meet, even though the question of what is the precise capacity is still open. Many of these bounds use at some point a bound on the number of codewords of length n of a certain q-ary Hamming weight r, which is the size of the Hamming ball of radius r, and the standard known result is that this size is $q^{nH_q(r/n)}$ to first order in the exponent, where $H_q(\cdot)$ is the q-ary entropy function.

There are other metrics of practical and mathematical interest, for example the Lee metric, introduced in [7], [8]. This metric is known to be suited to phase modulation schemes [2], and has more recently been used in multi-dimensional burst-error correction [9], constrained and partial response channels [10], interleaving schemes [11], and error correction for flash memories [12].

B. Prior work

Given a bound on the volume of the q-ary Lee ball of radius t, $V_t^{(n)}$, for a code of blocklength n, Chiang and Wolf [1] give the Hamming bound

$$V_{(d-1)/2}^{(n)} \leq q^{n(1-R(d))} \tag{1}$$

and the Gilbert-Varshamov bound,

$$V_d^{(n)} > q^{n(1-R(d))} \tag{2}$$

on the rate $R(d)$ for a code of minimum distance d in the Lee metric. They also give the following bound analogous to the singleton bound for a linear code of length n and rank k in the Lee metric,

$$d \leq \begin{cases} \frac{q+1}{4}(n-k+1) & \text{for odd } q \\ \frac{q^2}{4(q-1)}(n-k+1) & \text{for even } q \end{cases} \tag{3}$$

and the following method of calculating the volume of a sphere in the Lee metric

$$V_r^{(n)}(z) = \left(\sum_{i=0}^{r} \frac{1}{i!} \frac{d^i}{dz^i} A^{(n)}(z) \right)_{z=0} \tag{4}$$

which is mathematically involved. Here $A^{(n)}(z)$ is the generating function for the Lee metric.

Wyner and Graham [13] give the following Plotkin-type bound for the Lee metric: $d \leq \frac{n\overline{D}}{1-|C|^{-1}}$ where

$$\overline{D} = \begin{cases} \frac{q^2-1}{4q} & \text{for odd } q \\ \frac{q}{4} & \text{for even } q \end{cases} \tag{5}$$

and $|C|$ is the size of the code. Berlekamp [2] used a result due to Chernoff [14] to find the volume of a ball in the Hamming metric using the generating function as a starting point, but omits the corresponding calculations for the Lee metric as they are too tedious. He also gives a version of the Elias-Bassalygo bound for $0 < t < \overline{D}n$:

$$d \leq \left(\frac{t}{1-K^{-1}} \right) \left(2 - \frac{t}{n\overline{D}} \right) \tag{6}$$

where K is the least integer not less than $\frac{V_t^{(n)}}{q^{n(1-R)}}$, and t is chosen to minimize the RHS of the inequality.

Golomb [15] gave several results on spheres in several different discrete metrics.

Roth [16] also gives versions of the Hamming and Gilbert-Varshamov bounds for the Lee metric, and gives the following closed form expression for the volume of a Lee sphere of radius $t < \frac{q}{2}$ (here $\binom{t}{i} = 0$ if $i > t$).

$$V_t^{(n)} = \sum_{i=0}^{n} 2^i \binom{n}{i} \binom{t}{i} \tag{7}$$

As an exercise, he also includes the result that his expression is a strict lower bound for all $t \geq \frac{q}{2}$.

C. Our contributions

We develop a general technique based on the generating function of a metric and Sanov's theorem to find the volume of a sphere of a given radius. We show that this method allows us to recover the familiar bounds on the volume of a Hamming ball. We find upper and lower bounds on the volume of a ball in the Lee metric, and we use this result to find bounds analogous to the Hamming, Elias-Bassalygo and Gilbert-Varshamov bounds for the Lee metric.

D. Structure of the paper

In section II, we introduce the necessary notation. In section III we describe the general method using Sanov's theorem, and we give specific examples of it's use in section IV - the Hamming metric in section IV-A and the Lee metric in section IV-B. Finally, in section V, we use the results developed in the section IV-B to find Hamming and Gilbert-Varshamov bounds for the Lee metric.

II. Problem Setup and Notation

We adopt a slightly modified version of the notation and terminology of Berlekamp [2]. The discrete metric under consideration gives the distance between any two points in the space of n-length vectors over an alphabet of q symbols. Given a center C and a radius r, define the sphere $\mathcal{S}(C, t)$ as the set of all points whose distance from C is less than or equal to t. The surface area of such a sphere is the number of vectors whose distance from C is exactly t and it is denoted by $A_t^{(n)}$. The volume of such a sphere is the number of vectors whose distance from C is $\leq t$, and it is denoted as $V_t^{(n)}$. Clearly, we have the equality $V_t^{(n)} = \sum_{j=0}^{t} A_j^{(n)}$. Now, let $A^{(n)}(z) = \sum_j A_j^{(n)} z^j$, the generating function for the $A_j^{(n)}$. Since the distance is additive over the n coordinates, the generating function is multiplicative over these coordinates, and we have the equality $A^{(n)}(z) = [A^{(1)}(z)]^n$, where $A^{(1)}(z)$ gives the weights for a single symbol only. For example, for the Hamming metric we have $A^{(1)}(z) = 1 + (q-1)z$, and for the Lee metric we have

$$A^{(1)}(z) = \begin{cases} 1 + 2z + 2z^2 + \ldots + 2z^{\frac{q-1}{2}} & \text{for odd } q \\ 1 + 2z + 2z^2 + \ldots + 2z^{\frac{q-2}{2}} + z^{\frac{q}{2}} & \text{for even } q \end{cases} \tag{8}$$

III. The general method

We now describe a generalised method that works for any metric before going into specific examples. For any $A^{(1)}(z)$, we get a random variable X as follows: if $A^{(1)}(z)$ contains a term of the form $\alpha(j)z^i$, then the random variable X takes value j with probability $\frac{\alpha(j)}{q}$. It can be verified that this random variable is properly normalized. From the ideas introduced in the previous section, we can write $A^{(n)}(z) = \sum_j A_j^{(n)} z^j = [A^{(1)}(z)]^n$. Dividing both sides of the equation by q^n, we get that

$$\left[\frac{A^{(1)}(z)}{q}\right]^n = \sum_j \frac{A_j^{(n)}}{q^n} z^j = \sum_j B_j^{(n)} z^j \tag{9}$$

where $B_j^{(n)} := \frac{A_j^{(n)}}{q^n}$ Now, consider n i.i.d. random variables $X_1, \ldots, X_n$, each distributed as the random variable X defined above. We have, for each k,

$$\mathbb{P}\left[\sum_{j=0}^{n} X_j = k\right] = B_k^{(n)} \tag{10}$$

Therefore, to calculate a bound on the quantity $\sum_{j \leq k} B_j^{(n)}$, we need a bound on the quantity $\sum_{j \leq k} \mathbb{P}\left[\sum_{i=0}^{n} X_i = j\right]$, which we can calculate using Sanov's theorem. Multiplying the bounds that we obtain by q^n immediately gives bounds on $V_t^{(n)}$. The theorem states that [17]

Theorem 1 (Sanov's Theorem). *Let $X_1, X_2, \ldots, X_n$ be i.i.d. $\sim Q(x)$. Let $E \subseteq \mathcal{P}$ be a set of probability distributions and $\mathcal{P}$ be the set of all types from the n realisations $X_1, X_2, \ldots, X_n$. Then,*

$$Q^n(E) = Q^n(E \cap \mathcal{P}_n) \leq (n+1)^{|\mathcal{X}|} 2^{-nD(P^*||Q)} \tag{11}$$

where $|\mathcal{X}|$ is the support of each X_i, $D(\cdot||\cdot)$ is the K-L divergence, $Q^n(E)$ is the probability that the empirical distribution obtained from an n-long sample $X_1, \ldots, X_n$ each $\sim Q(x)$ belongs to the set E, and

$$P^* = \arg\min_{P \in E} D(P||Q) \tag{12}$$

is the distribution in E that is closest to Q in relative entropy. If we also have that the set E is the closure of its interior, then we also have the result

$$\frac{1}{n} \log Q^n(E) \to -D(P^*||Q) \tag{13}$$

Retaining terms upto first order in the exponent, we have

$$2^{-nD(P^*||Q) - o(n)} \leq Q^n(E) \leq 2^{-nD(P^*||Q) + o(n)} \tag{14}$$

Suppose that we want the expression for the volume of a ball of radius k, therefore we must first calculate the quantity $\sum_{j \leq k} \mathbb{P}\left[\sum_{i=0}^{n} X_i = j\right]$. To do this, we define the class E in Sanov's theorem to be the set

$$E := \{P \in \mathcal{P} : \mathbb{E}[X] \leq k/n\} \tag{15}$$

which is just compact notation for saying that we want the class of all n-length vectors such that the sum of terms is $\leq n$. In all of our applications of the theorem, the set E will be the closure of its interior, and the asymptotic result will hold.

In the rest of the paper, we will be interested in the volume of a sphere of radius pn, where p is some constant, and so the k/n in the final expression will be replaced by p. Also, we will be interested in $p < \overline{D}$, where $\overline{D}$ is the mean of the associated random variable X, because for $p > \overline{D}$, the class E starts containing the distribution Q, and the approach to the problem becomes different. Even the standard result [16] that the volume of the q-ary Hamming ball of radius pn is $q^{nH_q(p)}$ to first order in the exponent is only stated for $p < 1 - \frac{1}{q}$, which is precisely $\overline{D}$ in the q-ary Hamming metric.

We now need to minimize the relative entropy between two probability distributions, with constraints on the mean. This is a convex optimisation problem, and we can find the frame the problem and the dual in the general case. We omit the general case and see what it looks like in specific examples.

IV. Examples of the Bound

A. The Hamming metric

Applying the above for the Hamming metric is easy, because the class E is very easy to describe. For the Hamming metric,

$$A^{(1)}(z) = 1 + (q-1)z \tag{16}$$

which means that the associated random variable is

$$X = \begin{cases} 0 & \text{with probability } \frac{1}{q} \\ 1 & \text{with probability } \frac{q-1}{q} \end{cases} \tag{17}$$

The mean of this random variable is $\overline{D} = 1 - \frac{1}{q}$. If we are interested in the volume of a sphere of radius pn, where $p < \overline{D}$, the the class E contains all probability distributions with mean $\leq p$, and in this case consists of distributions of the form $(1-p', p')$ where $p' \leq p$. Using the fact that $1 - H(p)$ is an increasing function of p, it can be verified that the distribution in the class E that is closest to the random variable X in relative entropy is the distribution $(1-p, p)$, and substituting this in Sanov's theorem we get that

$$q^{-n(1-H_q(p))-o(n)} \leq Q^n(E) \leq q^{-n(1-H_q(p))+o(n)} \tag{18}$$

where $H_q(\cdot)$ is the q-ary entropy function. Multiplying this by q^n, we get that the size of a Hamming ball of radius pn is

$$q^{nH_q(p)-o(n)} \leq V_{pn}^{(n)} \leq q^{nH_q(p)+o(n)} \tag{19}$$

To first order in the exponent, this matches the standard result [16].

B. The Lee metric

For the Lee metric, we have that

$$A^{(1)}(z) = \begin{cases} 1 + 2z + 2z^2 + \ldots + 2z^{\frac{q-1}{2}} & \text{for odd } q \\ 1 + 2z + 2z^2 + \ldots + 2z^{\frac{q-2}{2}} + z^{\frac{q}{2}} & \text{for even } q \end{cases} \tag{20}$$

For odd q, the associated random variable is

$$X = \begin{cases} 0 & \text{with probability } \frac{1}{q} \\ 1, 2, \ldots, \frac{q-1}{2} & \text{each with probability } \frac{2}{q} \end{cases} \tag{21}$$

and for even q, the random variable is

$$X = \begin{cases} 0 & \text{with probability } \frac{1}{q} \\ 1, 2, \ldots, \frac{q-2}{2} & \text{each with probability } \frac{2}{q} \\ \frac{q}{2} & \text{with probability } \frac{1}{q} \end{cases} \tag{22}$$

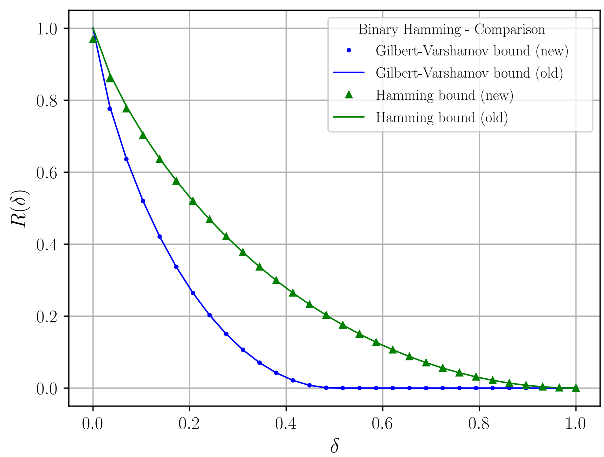

Fig. 1. The plots for the Hamming metric. The lines denote the known results, and the markers denote the results obtained from our techniques.

If we are interested in the volume of a sphere of radius pn, we again define the class E as containing all distributions with mean $\leq p$.

The following lemma is from [2].

Lemma 2. *The mean of the random variable X is the average distance between codewords in the Lee metric, and is given by*

$$\overline{D} = \begin{cases} \frac{q}{4} & q \text{ is even} \\ \frac{q^2-1}{4q} & q \text{ is odd} \end{cases} \tag{23}$$

We now need to minimize the relative entropy between a distribution $Y \in E$ and the random variable X. This is a convex optimisation problem.

$$\begin{aligned} \underset{\mathbb{P}_Y}{\text{minimize}} \quad & \sum_j \mathbb{P}_Y(j) \log \frac{\mathbb{P}_Y(j)}{\mathbb{P}_X(j)} \\ \text{subject to} \quad & \sum_j \mathbb{P}_Y(j) = 1 \\ & \mathbb{P}_Y(j) \geq 0 \ \forall j \\ & \sum_j j\mathbb{P}_Y(j) \leq p \end{aligned} \tag{24}$$

Note that this is completely independent of the blocklength. Taking the dual of this problem and simplifying the result obtained, we get the following linear program:

$$\begin{aligned} \underset{\lambda}{\text{maximize}} \quad & -p\lambda - \log\left(\sum_j \mathbb{P}_X(j) e^{-j\lambda}\right) \\ \text{subject to} \quad & \lambda \geq 0 \end{aligned} \tag{25}$$

Directly finding the maximising λ for each value of p, we get a numerical bound on the required size, which we show in Figure 1. We can also approximate the coefficients using a suitably centred and scaled Gaussian given by the central limit theorem, but this is a poor approximation more than a few standard deviations away from the central maxima.

We can also try to obtain analytical results by exploiting the fact that strong duality holds for this problem and any solution to the dual problem automatically implies an upper bound on the primal. Therefore, depending on the value of q, we can choose $\lambda(p)$ as a function of p and that can give some analytic bounds on the size.

To do this, observe that when $p = \overline{D}$, the distribution $Q(x)$ is a member of the set E and thus the distribution that minimizes relative entropy is the distribution Q itself. This happens for $\lambda = 0$, implying that that the function $\lambda(p)$ has a zero at $p = \overline{D}$.

We choose the function $\lambda(p) = c(q)(\overline{D}^{1/q} - p^{1/q})$, where $c(q)$ is a positive constant dependent on q only, and is chosen to give the closest fit to the actual function $\lambda^*(p)$[1]. Note that since $x^{1/q}$ is a mononotonically increasing function of x, for all $p < \overline{D}$, $\lambda(p) > 0$, which satisfies the requirement that $\lambda \geq 0$. The numerically obtained values of c for different values of q are given in the table I.

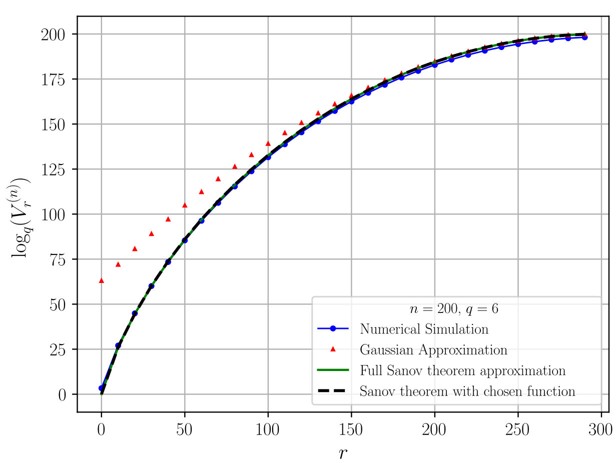

Fig. 2. Results of the Sanov theorem approximation compared to the actual value. Note the log scale on the y-axis. An approximation using the central limit theorem is also plotted for comparison. One can also see the near perfect match between the result of applying Sanov's theorem and the function defined.

V. Bounds on the Lee metric

Note that the results presented in the previous section imply that the volume of the Lee sphere of radius pn is lower bounded by

$$\log_q V_{pn}^{(n)} \geq n \left[1 + \frac{p\lambda(p) + \log\left(\sum_j \mathbb{P}_X(j) e^{-j\lambda(p)}\right)}{\log q} \right] - o(n) \tag{26}$$

[1]We observed the plot as shown in Figure 1 is not very sensitive to perturbations of $c(q)$ away from the optimal value. Also note that *any* value of $c(q)$ and *any* positive function $\lambda(p)$ is going to imply an upper bound on the optimal value of the primal linear program, so we can choose the functions as we wish. The given choices work very well.

TABLE I
Values of $c(q)$

q	$c(q)$	q	$c(q)$
4	6.7335	10	9.1297
5	7.5202	12	9.8138
6	7.6108	15	10.7921
7	8.1711	20	12.1588
8	8.3996	25	13.4049
9	8.8682	30	15.5390

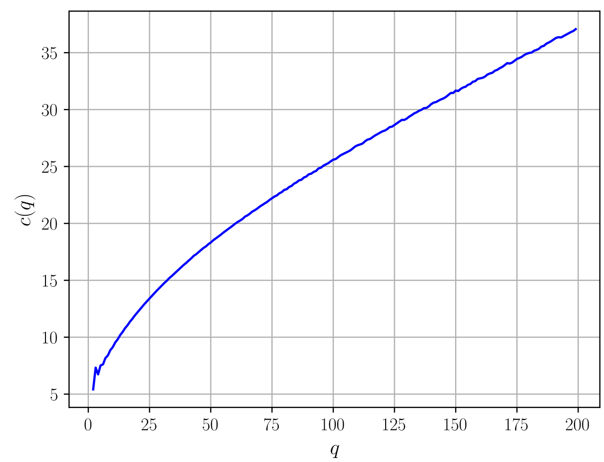

Fig. 3. Plot of $c(q)$ with respect to q

where $\lambda(p) = c(q)(\overline{D}^{1/q} - p^{1/q})$. There's also a very similar upper bound.

$$\log_q V_{pn}^{(n)} \leq n \left[1 + \frac{p\lambda(p) + \log\left(\sum_j \mathbb{P}_X(j) e^{-j\lambda(p)}\right)}{\log q} \right] + o(n) \tag{27}$$

We can use these bounds on the volume to find bounds on the possible rates of a code given the minimum distance criterion that the code must satisfy. We find such bounds in this section.

A. The Hamming Bound

Theorem 3 (Hamming bound for the Lee metric)**.** *The rate $R(\delta)$ of a code in the Lee metric with minimum distance δn is bounded above as*

$$R(\delta) \leq -\frac{\frac{\delta}{2}\lambda(\frac{\delta}{2}) + \log\left(\sum_j \mathbb{P}_X(j) e^{-j\lambda(\frac{\delta}{2})}\right)}{\log q} + o(1) \tag{28}$$

Proof. The proof follows immediately by substituting $p = \frac{\delta}{2}$ in the expression for the bound on the volume of the Lee sphere (equation (26)) and then using equation (1). □

B. The Gilbert-Varshamov Bound

Theorem 4 (Gilbert-Varshamov bound for the Lee metric)**.** *The optimal rate $R(\delta)$ of a code in the Lee metric with* *minimum distance δn is bounded below as*

$$R(\delta) \geq -\frac{\delta\lambda(\delta) + \log\left(\sum_j \mathbb{P}_X(j)e^{-j\lambda(\delta)}\right)}{\log q} - o(1) \qquad (29)$$

Proof. The proof follows immediately by substituting $p = \delta$ in the expression for the bound on the volume of the Lee sphere (equation (26)) and then using equation (2). □

C. The Elias-Bassalygo Bound

Using the general form of the EB bounds given, for example, in [2], theorem 13.67, we get

Theorem 5 (Elias-Bassalygo bound for the Lee metric)**.** *The rate optimal $R(\delta)$ of a code in the Lee metric with minimum distance δn is bounded below as*

$$R(\overline{\delta}) \leq -\frac{\overline{\delta}\lambda(\overline{\delta}) + \log\left(\sum_j \mathbb{P}_X(j)e^{-j\lambda(\overline{\delta})}\right)}{\log q} + o(1) \qquad (30)$$

where $\overline{\delta} = \overline{D}\left(1 - \sqrt{1 - \frac{\delta}{\overline{D}}}\right)$

Proof. The proof follows after some simplification from the general expression and by substituting $p = \overline{\delta}$ in the expression for the bound on the volume of the Lee sphere ((26)). □

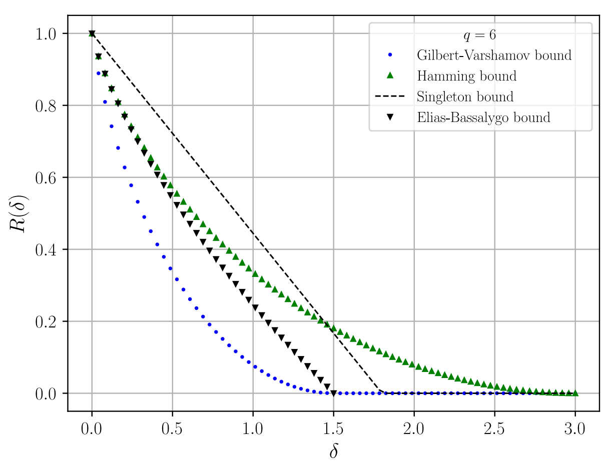

Fig. 4. The various bounds for the Lee metric. The Hamming, Gilbert-Varshamov and Elias-Bassalygo bounds are the results that we derive, and the singleton bound is from [1]. It is interesting to note that, like in the Hamming case, the singleton, the EB and GV bounds agree on the zero-rate point at $\delta = \overline{D}$. The EB bound is again the tightest upper bound.

VI. Conclusion

We have used Sanov's theorem and convex optimisation techniques to obtain estimates on the volume of a Lee ball and we then used it to obtain bounds on possible rates in the Lee metric. We now look at some possible directions of future work. Using the function $\lambda(p)$ that we defined, we were able to obtain a solution for the volume of a Lee sphere in terms of a summation. Whether we can obtain a closed form bound by possibly weakening it a little is still an open question. Also, the final convex optimisation problem in the case of the Lee metric is a maximisation over a single variable only, and as such should be solvable using calculus. However, the resulting equations are intractable. Also, we have included a plot that shows how well our function approximates the actual solution of that problem. We leave open the question of whether the solution of the equations obtained if we try to find the maxima by taking a derivative leads naturally to a function of the form we have used.

Also, we have given Hamming and Gilbert-Varshamov bounds for the Lee metric. A bound analogous to the MRRW bound for the Lee metric remains open.

Acknowledgment

We thank Prof Sidharth Jaggi of the Chinese University of Hong Kong (CUHK) for bringing bounds on the Lee metric to our attention and for several insightful discussions.

References

[1] J. C.-Y. Chiang and J. K. Wolf, "On channels and codes for the Lee metric," *Information and Control*, vol. 19, no. 2, pp. 159 – 173, 1971. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0019995871907911

[2] E. R. Berlekamp, *Algebraic Coding Theory - Revised Edition*. River Edge, NJ, USA: World Scientific Publishing Co., Inc., 2015.

[3] M. Plotkin, "Binary codes with specified minimum distance," *IRE Transactions on Information Theory*, vol. 6, no. 4, pp. 445–450, Sep. 1960.

[4] L. A. Bassalygo, "New upper bounds for error-correcting codes," *Problemy Peredači Informacii*, vol. 1, no. vyp. 4, pp. 41–44, 1965.

[5] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch, "New upper bounds on the rate of a code via the delsarte-macwilliams inequalities," *IEEE Transactions on Information Theory*, vol. 23, no. 2, pp. 157–166, March 1977.

[6] E. N. Gilbert, "A comparison of signalling alphabets," *The Bell System Technical Journal*, vol. 31, no. 3, pp. 504–522, May 1952.

[7] C. Y. Lee, "Some properties of nonbinary error-correcting codes," *IRE Trans. Information Theory*, vol. 4, pp. 77–82, 1958.

[8] W. Ulrich, "Non-binary error correction codes*," *Bell System Technical Journal*, vol. 36, no. 6, pp. 1341–1388, 1957. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1957.tb01514.x

[9] T. Etzion and E. Yaakobi, "Error-correction of multidimensional bursts," *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 961–976, March 2009.

[10] R. M. Roth and P. H. Siegel, "Lee-metric BCH codes and their application to constrained and partial-response channels," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1083–1096, July 1994.

[11] M. Blaum, J. Bruck, and A. Vardy, "Interleaving schemes for multidimensional cluster errors," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 730–743, March 1998.

[12] A. Barg and A. Mazumdar, "Codes in permutations and error correction for rank modulation," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3158–3165, July 2010.

[13] A. D. Wyner and R. L. Graham, "An upper bound on minimum distance for a k-ary code," *Information and Control*, vol. 13, no. 1, pp. 46–52, 1968. [Online]. Available: https://doi.org/10.1016/S0019-9958(68)90779-1

[14] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *Ann. Math. Statist.*, vol. 23, no. 4, pp. 493–507, 12 1952. [Online]. Available: https://doi.org/10.1214/aoms/1177729330

[15] S. Golomb, "A general formulation of error matrices (corresp.)," *IEEE Transactions on Information Theory*, vol. 15, no. 3, pp. 425–426, May 1969.

[16] R. Roth, *Introduction to Coding Theory*. New York, NY, USA: Cambridge University Press, 2006.

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. New York, NY, USA: Wiley-Interscience, 2006.